Auditorías a las estrategias de ciberseguridad

Breve descripción:

Este componente formativo aborda aspectos clave de las estrategias de seguridad de los activos más importantes para las organizaciones. Con su estudio responsable, el aprendiz se afianzará en lo relacionado con enfoques y cambios para seguridad, prevención de incidentes de ciberseguridad, atención, programas de auditoría y monitoreo efectivo.

Junio 2023

Tabla de contenido

Introducción

Aquí inicia el estudio del componente formativo “Auditorías a las estrategias de ciberseguridad”. En este punto, visualice con atención el video que se muestra en seguida y comience esta experiencia de aprendizaje, en la que se le desean todos los éxitos.

¡Adelante!

Video 1. Auditorías a las estrategias de ciberseguridad

Enlace de reproducción del video

Síntesis del video: Auditorías a las estrategias de ciberseguridad
Dentro del ciclo que enmarca la norma ISO/IEC 27001:2013, se establece una fase que permite evaluar el rendimiento del sistema de seguridad de la información y, en especial, los controles que fueron propuestos para mejorar la seguridad de los activos de información de la organización. Esta fase implica establecer una métrica, con la cual se identifiquen los rangos de valores aceptables y no aceptables, de cada control. A partir de esta evaluación se podrán establecer los mecanismos de mejora de los mismos controles, o de cambio completo de un determinado control, en caso de ser necesario. “Lo que no se mide no se puede mejorar. Lo que no se mejora, se degrada siempre”. William Thomson Kelvin Se considera que la evaluación de la estrategia de seguridad debe realizarse de manera periódica, convirtiéndose en punto de partida para la adopción de la mejora continua. Con el estudio de este componente formativo, usted estará en capacidad de reconocer aspectos importantes de la evaluación de las estrategias de ciberseguridad y su aplicación. De la misma manera, obtendrá elementos básicos para la realización de un informe de auditoría sobre la operación de la estrategia de ciberseguridad. El proceso de ejecución de la evaluación de estrategia de ciberseguridad implica, entre otros aspectos, estimar el diagnóstico, el diseño, la aplicación y el monitoreo de la operación de la misma; todo ello, adoptando lineamientos de la

metodología de pruebas de efectividad, que son una serie de actividades de suma importancia que ayudarán a medir y/o comprobar la eficiencia del modelo de seguridad, que tengan las organizaciones.

De esta misma manera, se requiere la realización de un informe basado en la auditoría, ya que este aportará el compendio de vulnerabilidades que puede tener la organización, a nivel informático.

1. La auditoría cibernética

A medida que las organizaciones adoptan nuevas tecnologías digitales, aumenta el riesgo de ser objeto de ciberataques. La mayor complejidad de la red que surge como resultado de la innovación digital, a menudo crea nuevas brechas en la red para que las exploten los ciberadversarios.

Si no se controlan, estos riesgos pueden socavar los objetivos organizacionales, por lo que es fundamental que las empresas cuenten con programas efectivos de ciberseguridad.

Se debe tener presente que:

- Un componente clave para el éxito de estos programas es la administración de auditorías de ciberseguridad.
- La administración periódica de auditorías de ciberseguridad ayuda a las organizaciones a identificar brechas en su infraestructura de ciberseguridad.
- Las organizaciones también pueden utilizar las auditorías para evaluar su cumplimiento de diversas leyes y reglamentos.
- Con un programa de auditoría de seguridad cibernética establecido, las empresas pueden monitorear de manera efectiva su postura de seguridad a medida que sus redes crecen y se vuelven más complejas.

1.1. Técnicas de auditoría

Las auditorías son un “proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas, de manera objetiva, con el fin de determinar el grado en que se cumplen los criterios de auditoría” (ISO, 2018). Las auditorías se convierten en el proceso mediante el cual se valida y corrobora, con algún proceso de observación, indagación o verificación, si un criterio de evaluación se está cumpliendo, de acuerdo a los parámetros establecidos.

1.2. Tipos de auditoría

De acuerdo al momento en que se realiza la auditoría, del alcance de la misma y del auditor que la realiza, estas se pueden clasificar en 3 tipos: de primera parte, de segunda parte o de tercera parte (ISO, 2018):

a) Auditoría de primera parte.
   - Auditoría interna.

b) Auditoría de segunda parte:
   - Auditoría externa de proveedor.
   - Otra auditoría externa de parte interesada.

c) Auditoría de tercera parte:
   - Auditoría de certificación y/o acreditación.
   - Auditoría legal, reglamentaria o similar.

Pero, ¿cuáles son las especificidades de cada tipo de auditoría? Aquí se los presentamos; explore el recurso que se muestra enseguida y descúbralo; le sugerimos tomar nota de ello en su libreta personal de apuntes. ¡Adelante!

Figura 1. Tipos de auditoría

1.3. Definiciones y elementos fundamentales de la auditoría

Para establecer o entender un ejercicio de auditoría es necesario referirse a la norma GTC-ISO 19011:2018, la cual establece las directrices para la auditoría de los sistemas de gestión.

Entérese de algunas definiciones y lineamientos que da la norma y que aseguran que el proceso de evaluación y auditoría del sistema de gestión de seguridad de información, en las organizaciones, sea efectivo:

Video 2. Definiciones y elementos fundamentales de la auditoría

Enlace de reproducción del video

Síntesis del video: Definiciones y elementos fundamentales de la auditoría
Se presentan las definiciones y elementos de la auditoría según la norma GTC-ISO 19011:2018: el criterio de auditoría, la evidencia objetiva, el alcance de auditoría, el plan de auditoría, la evidencia de auditoría y los hallazgos de auditoría.

1.4. Consideraciones importantes para una auditoría

De acuerdo a la norma GTC-ISO 19011:2018, una auditoría de sistemas de gestión se debe establecer bajo ciertas condiciones que permitan la construcción y desarrollo de la misma, en la organización.

Le invitamos a revisar con especial atención las consideraciones, sobre la auditoría, contenidas en el siguiente video.

Video 3. Definiciones Consideraciones importantes para la auditoría

Enlace de reproducción del video

Síntesis del video: Consideraciones importantes para la auditoría
Las auditorías de los sistemas de gestión de la seguridad de la información deben ser establecidas, teniendo en cuenta algunas condiciones que favorecerán rotundamente tanto a su construcción como a su desarrollo. Las organizaciones deben prestar especial atención a la manera en que se estructura, programa y organiza la auditoría, lo cual desencadenará en aseguramiento no solo de información, sino en garantizar la calidad y el cumplimiento de sus procesos, actividades y productos.

1.5. Principios de la auditoría

Entiéndase como principios de auditoría a los elementos y aspectos fundamentales, para desarrollar un ejercicio de auditoría y obtener resultados confiables, objetivos, pertinentes y suficientes para que la organización tome las decisiones apropiadas en el futuro.

Adicional de las técnicas, tipos, definiciones y consideraciones, relacionadas con el proceso de auditoría, hay que tener en cuenta que toda acción en pos de la auditoría, ha de estar orientada por estos principios. Conózcalos a continuación:

- **Integridad.** El auditor debe realizar el ejercicio a partir de su honestidad, imparcialidad, diligencia y responsabilidad, durante toda la auditoría.

- **Presentación ecuánime.** Los resultados de la auditoría deben reflejar la veracidad y exactitud de la información que se pudo evaluar durante la auditoría.
- **Debido cuidado profesional.** El auditor debe tener la capacidad de formular juicios de valor razonables durante toda la auditoría.
- **Confidencialidad.** La seguridad de la información, durante el ejercicio de la auditoría, es un factor de sumo cuidado. Se debe garantizar que la información, su uso y protección, serán aplicados de manera apropiada.
- **Independencia.** El auditor se debe considerar y sentir independiente y libre de sesgo y conflicto de intereses, durante todo el ejercicio de la auditoría, lo cual permite realizar una evaluación objetiva.
- **Enfoque basado en la evidencia.** Los criterios evaluados deben contar con la presentación y verificación de las evidencias correspondientes, lo cual da fe del ejercicio de auditoría dando fiabilidad a esta.

¡Importante!

Con los anteriores principios, se busca objetividad, confianza y contar con un insumo para identificar el rendimiento de la estrategia de seguridad de la información y poder tomar decisiones.

1.6. Fases de la auditoría

De acuerdo al diagrama de flujo presentado por la metodología de la norma GTC-ISO 19011:2018, se pueden establecer tres fases para el desarrollo de una auditoría: la planeación, la implementación y el monitoreo de la misma.

Explore el recurso didáctico que se muestra a continuación y profundice en las fases de la auditoría. Le recordamos que puede llevar registro de los aspectos más destacados, en su libreta personal de apuntes.

a) Planeación de la auditoría

- La auditoría debe ser programada, aprobada e informada a todos los líderes de procesos e interesados con tiempo de antelación.
- Para las auditorías, es necesario que todos los líderes de procesos y equipos estén informados y alineados en atención a los requerimientos de los auditores, de tal manera que pueda ser presentada cualquier evidencia o requerimiento que sea solicitado por el auditor.
- De acuerdo con el ciclo PHVA, las auditorías deben de realizarse por lo menos una vez en el año, aunque si la organización considera, debido a la criticidad de sus procesos, o con el fin de determinar alguna verificación, que deban hacer más en este periodo de tiempo, también es válido; esto ayudaría a evaluar e identificar falencias en los criterios de auditoría.
- Para cada auditoría se debe contar con los informes de las auditorías anteriores, tanto internas como externas, y revisiones de la alta dirección. Además, estas auditorías deben realizarse antes de las auditorías de certificación y/o acreditación, ya que estas auditorías internas pueden detectar falencias que pueden corregirse para dicha evaluación.

b) Implementación de la auditoría

- En este evento se realiza la apertura de la auditoría en la cual se presenta la metodología, tiempos, procesos, sistemas o cualquier detalle que permita identificar el alcance de la misma, se hace entrega de la información existente o de auditorías anteriores, y se da inicio al ejercicio de acuerdo a la programación establecida.
- Una vez se finalice el ejercicio, el auditor realiza el informe, el cual es presentado durante el cierre de la auditoría.
- Con el informe del auditor, la alta dirección establecerá las acciones de mejora a futuro, a través de un plan de mejoramiento; estas acciones pueden ser correctivas, preventivas o de mejora.

c) Monitoreo a la auditoría

- En esta fase, se busca realizar el seguimiento a las acciones establecidas en el último ejercicio, con el fin de validar su efectividad en la corrección de falencias o la adecuada implementación de nuevos controles.
- Este seguimiento debe realizarse de manera permanente con el fin de reportar avances y fortalecer aquellas acciones que pueden retrasar el cumplimiento de los objetivos.

2. Pruebas de vulnerabilidad cibernética

Las empresas se enfrentan a una amplia gama de amenazas de ciberseguridad al volverse más dependientes de internet, el acceso remoto y la tecnología en general. Para mantener seguros sus datos y aplicaciones esenciales, deben identificar las vulnerabilidades potenciales que los ciberdelincuentes podrían explotar en nombre de sus objetivos.

Mediante el uso de una combinación de herramientas de prueba de vulnerabilidades y técnicas de escaneo, los expertos en seguridad cibernética pueden ayudarlos a identificar y reforzar las brechas y debilidades de seguridad.

¡Importante!

Es una práctica común que los entornos de desarrollo y prueba para los sistemas de aplicaciones comerciales, la mayoría de las veces también contengan datos confidenciales del cliente, que se utilizan para desarrollar, simular y probar la lógica del código de la aplicación.

¡Atención!

Esto implica que estos entornos de prueba, que no son de producción, también deban protegerse de la misma manera que el entorno de TI de producción.

2.1. Finalidad de las pruebas

El enfoque de las pruebas de efectividad, frente a la metodología, es comprobar o medir la eficiencia de la ejecución del modelo de seguridad en organizaciones. Con el

fin de ayudar a las organizaciones se han desarrollado metodologías que favorecen la comprensión y el desarrollo de las pruebas, el alcance de objetivos y el beneficio que se gana al identificar sus etapas y gestionarlas.

Tales metodologías se desarrollan en diferentes etapas, ayudando a definir qué tanto ha avanzado la organización con la implementación del modelo. Así pues, por medio de la valoración de diferentes aspectos, se podrán identificar también vulnerabilidades y amenazas, a las cuales está expuesta la organización, de igual manera que las debilidades de los controles implementados.

A continuación, explore el recurso didáctico con el que le presentamos las etapas del procedimiento de las pruebas, según lo estipulado por la Guía metodológica de pruebas de efectividad, del MINTIC:

Video 4. Finalidad de las pruebas

Enlace de reproducción del video

Síntesis del video: Finalidad de las pruebas
Se recopila toda la información para dar inicio a la actividad, donde se identificarán los activos de mayor importancia, conocer el contexto de la entidad, etapa de revisiones de manuales y etapa de identificación de amenazas.

2.2. Pruebas y análisis

Mediante las pruebas y análisis, las entidades identifican los diferentes riesgos que se muestran por las debilidades en la implementación del modelo de seguridad y de privacidad de la información y las vulnerabilidades que se manifiestan dada la ausencia de controles de seguridad que logren mitigar riesgos.

Este tipo de pruebas están orientadas a la evaluación de la estructura de seguridad de la organización; para ello, las organizaciones han de revisar diferentes frentes de trabajo como, por ejemplo, el Anexo A de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel y estado de madurez de la organización en correspondencia con los niveles expuestos en el modelo de seguridad y privacidad y las recomendaciones para que la organización logre plasmar el concepto de Ciberseguridad.

2.3. Tipos de pruebas de efectividad

Respecto de los tipos de pruebas de efectividad, se pueden realizar tres tipos, basados en el nivel de conocimiento del entorno o de la infraestructura de la organización objetivo.

Estos tres tipos de prueba son:

- **Pruebas con conocimiento nulo del entorno.** Se trata del tipo de prueba en la que simulará a un atacante real, ya que se basa en que cuenta con muy poco conocimiento o quizá nulo conocimiento del objetivo o su infraestructura.
- **Pruebas con conocimiento medio del entorno.** Se refiere a cuando, para la prueba de "pentesting", se cuenta con más información sobre aquel ambiente que será atacado, es decir, direcciones IP, sistemas operativos, arquitectura de red etc. De igual manera es información limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma.
- **Pruebas con conocimiento completo del entorno.** Son pruebas en donde el hacker cuenta con toda la información disponible y relacionada con el sistema objetivo del ataque. Por lo general, son para asuntos de auditoría.

2.4. Procedimiento de ejecución de pruebas de efectividad

Las pruebas de efectividad pueden realizarse por medio de las siguientes acciones de manera secuencial: contextualización, reconocimiento del objetivo,

modelado de amenazas, evaluación de vulnerabilidades, explotación, postexplotación y reporte.

A continuación, se especifican las acciones con las que se aplican las pruebas de efectividad; comprenda los aspectos importantes de cada una de ellas y lleve registro en su libreta personal de apuntes:

- **Contextualización.** Esta acción se basa en identificar los alcances reales de las pruebas y de los procedimientos a ejecutar con base a las necesidades identificadas.
- **Reconocimiento de objetivo.** Esta acción, busca obtener tanta información del objetivo como sea posible para poder ser empleada en la acción de evaluación de vulnerabilidades y la acción de explotación.
- **Modelado de amenazas.** Esta acción establece la relación entre el atacante y el activo intentando definir el beneficio que puede alcanzar el atacante si logra penetrar el sistema y afectar la información de alguna manera.
- **Evaluación de vulnerabilidades.** Es la acción que descubre falencias en los sistemas y aplicaciones, que pueden llegar a ser aprovechados por un atacante.
- **Explotación.** Es la acción que busca, concretamente, acceder al sistema, apalancando las debilidades identificadas en la etapa anterior o sobrepasando los controles de seguridad existentes.
- **Postexplotación.** Acción que busca identificar el tipo de información que se puede obtener, a qué otros sistemas de información se puede ingresar desde el sistema capturado, las opciones de configuración, información de

red, todo esto con el objetivo principal de determinar el valor de la máquina para la organización.

- **Reporte.** Acción con la que se documentan resultados obtenidos en cada anterior acción.

De la aplicación procedente, responsable y oportuna de las pruebas, depende en gran medida su efectividad y su potencial aprovechamiento. Las pruebas de efectividad han de realizarse con las acciones mencionadas, siendo cada una de estas, una acción vinculada consecuentemente con las anteriores o con las posteriores.

Para ahondar en los aspectos importantes relacionados con pruebas de efectividad y su procedimiento, le recomendamos estudiar la Guía No 1. Guía metodológica de pruebas de efectividad del MinTIC.

2.5. Alcance de las pruebas

Deberán existir una serie de reglas y otros elementos importantes para la aplicación de las pruebas de efectividad técnicas, con el fin de asegurar que tales actividades no lleguen a incurrir en fallas mayores y que, también, sea posible la afectación de la infraestructura o de las distintas operaciones de la organización.

Dentro del alcance, es posible definir aspectos como los que se especifican en el recurso que se muestra a continuación:

Figura 2. Aspectos dentro del alcance

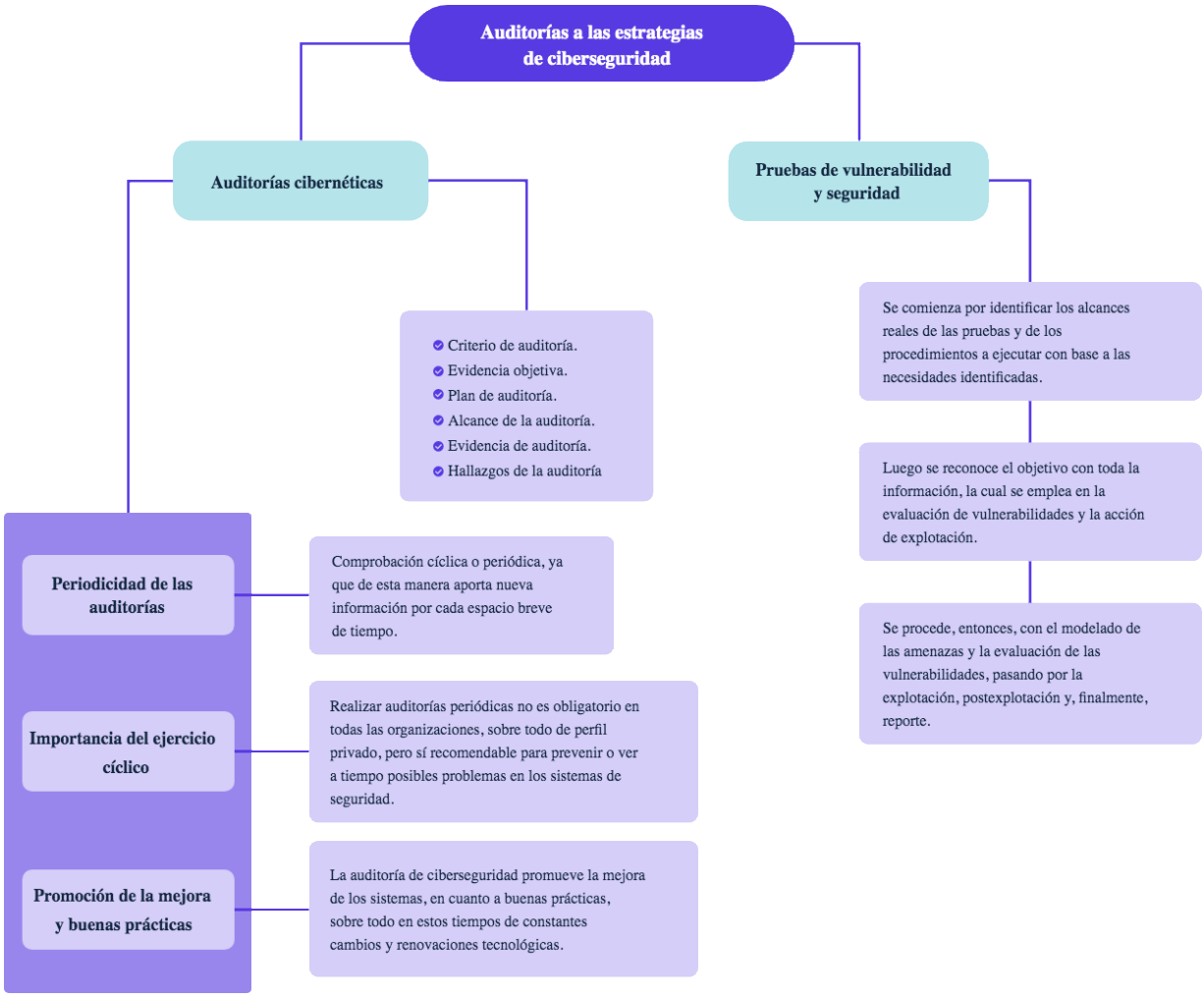
¡Importante!

Estos alcances permitirán controlar internamente el desarrollo de las pruebas, así como manejar los acuerdos de servicio con terceros que pueden llegar a realizar estos procedimientos.

Síntesis

Con este punto, se finaliza el estudio de los contenidos de este componente formativo. Es momento de hacer síntesis, para lo cual se debe analizar el esquema que se muestra a continuación y registrar esta síntesis en la libreta personal de apuntes. Además, se deben repasar los temas que considere necesario.

¡Adelante!



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Procedimiento de ejecución de pruebas de efectividad.	Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Guía metodológica de pruebas de efectividad.	Guía técnica	https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf
Principios de la auditoría	Organización Internacional de Normalización (2013). Seguridad de la información, ciberseguridad y protección de la privacidad. (ISO 27001). ISO.	Norma técnica	https://www.iso.org/standard/54534.html

Glosario

Atributo: cualquier propiedad o característica que permite distinguir un objeto de otro.

Auditoría: proceso de verificación y/o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas.

Auditoría externa: auditoría realizada por compañías independientes de la organización o aquellas que son realizadas por personas ajenas a la empresa, contratadas para ello.

Escala: rango de valores organizados con los cuales se evalúa un atributo.

Evidencia: información suficiente que respalda alguna acción.

Indicador: unidad que permiten medir el desempeño o desarrollo de alguna acción o de algún control.

Métrica: conjunto de criterios y condiciones necesarios para medir un control o una acción.

Modelado de amenazas: acción que establece la relación entre el atacante y el activo intentando definir el beneficio que puede alcanzar el atacante si logra penetrar el sistema y afectar la información de alguna manera.

Pruebas de efectividad: acciones que se enfocan en establecer una línea base del estado de seguridad de la organización, con el fin de facilitar la identificación de la brecha en la implementación del modelo de seguridad.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Referencias bibliográficas

Avansis (2020). Auditoría de ciberseguridad. Avansis.

Ciberseguridad y Riesgos Digitales (2020). Normas ISO en auditoría informática: Cuáles son las más importantes. Ealde. https://www.ealde.es/iso-auditoria-informatica/

Instituto Nacional de Ciberseguridad. (2015). Protección de la información. Incibe. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

ISO (2020). Evaluación del desempeño en ISO 27001. (ISO 27001). ISO. https://normaiso27001.es/evaluacion-del-desempeno-en-iso-27001/

ISO (2020). Fase 8 auditoría interna según ISO 27001. (ISO 27001). ISO. https://normaiso27001.es/fase-8-auditoria-interna-segun-iso-27001/

ISO (2018). Directrices para la auditoría de los sistemas de gestión. (ISO 19011). ISO. https://cmdcertification.com/wp-content/uploads/2020/11/ISO-19011-2018.pdf

Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Guía de auditoría. Ministerio de Tecnologías de la Información y Comunicaciones. https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Guía metodológica de pruebas de efectividad. Ministerio de Tecnologías de la Información y Comunicaciones. https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Organización Internacional de Normalización (ISO, 2013). Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. https://www.iso.org/standard/54534.html

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Líder del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Ronald Alexander Vacca Ascanio	Experto Temático	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Carolina Coca Salazar	Asesor Metodológico	Centro de Diseño y Metrología - Regional Distrito Capital
José Gabriel Ortiz Abella	Corrector de Estilo	Centro de Diseño y Metrología - Regional Distrito Capital
Yerson Fabián Zarate Saavedra	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Desarrollador Full-Stack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Eduardo Garavito Parada	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
María Carolina Tamayo López	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruíz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander